ABSTRACT

According to one embodiment, computer system is disclosed. The computer system includes a central processing unit (CPU), and a chipset coupled to the CPU including protected registers and a host controller. The computer system also includes a bus coupled to the host controller and a peripheral device coupled the bus. Trusted software accesses the protected registers to transmit encrypted data between the host controller and the peripheral device upon startup of the computer system to verify that the peripheral device is trustworthy.